HMM Sequential Hypothesis Tests for Intrusion Detection in MANETs
Extended Abstract

Alvaro A. Cardenas, Vahid Ramezani, John S. Baras
Department of Electrical and Computer Engineering and
Institute for Systems Research
University of Maryland
College Park, MD, 20740
USA

Abstract

Most of the work for securing the routing protocols of mobile ad hoc wireless networks has been done in prevention. Intrusion detection systems play a complimentary role to that of prevention for dealing with malicious insiders, incorrect implementation and attack models. We present a statistical framework that allows the incorporation of prior information about the normal behavior of the network and of network attacks in a principled way for the detection of known and unknown attacks. For detecting an attack as soon as possible we use quickest change detection algorithms. We use hidden Markov models (HMMs) as a generative view of the dynamic evolution of the hop count distribution. Our results show that simple attacks can be detected by an anomaly detection framework. However, detection of more complex attacks requires incorporation of prior knowledge in the HMMs.

1 Introduction

Mobile -wireless- ad hoc networks (MANETs) are particularly vulnerable to attacks on their routing protocols. Unlike fixed networks, the routers usually do not reside in physically protected places and can fall under the control of an attacker more easily. This insider can then advertise or forward incorrect routing information. Furthermore the wireless medium makes it easier for an outsider to eavesdrop and inject fake messages. With the injection of fabricated messages an attacker can modify the normal route establishment of the network without the need to compromise any nodes.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **2003**	2. REPORT TYPE	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **HMM Sequential Hypothesis Tests for Intrusion Detection in MANETs Extended Abstract**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Research Office,PO Box 12211,Research Triangle Park,NC,27709**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **10**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

1.1 Routing attacks

An attacker who gets access to a node in the network can mount several attacks. She can disrupt the flow of the network by dropping, corrupting or delaying the packets passing through the compromised node. Furthermore the attacker can fabricate packets with incorrect information such as packet generation with fake source address, and can also modify the routing packets by advertising false routes. A selfish node trying to avoid being used as a router can falsely claim longer distances to other nodes, or they can try to attract as much traffic as possible (a blackhole attack) by advertising short distances to all destinations or by a sequence number rushing attack.

One of the attacks exploiting the wireless medium is the wormhole attack. In this case an attacker records packets or bits at one location in the network and tunnels them to another location by means of a single long-range directional wireless link or through a direct wired link to a colluding attacker. At the end of the tunnel certain packets are retransmitted into the network. The wormhole attack can be devastating to a routing protocol. For example in DSDV if each routing advertising sent by node A were tunneled to node B (and any data packet is not retransmitted) and vice versa, then A and B would believe that they are neighbors. If they were not within wireless transmission range, they would be unable to communicate. Furthermore, if the best existing route from A to B were at least 2n+2 hops long, then any node within n hops of A would be unable to communicate with B and vice versa [1].

1.2 The role of intrusion detection in security

In order to provide reliable routing we must design security mechanisms for MANETs. There are three main design considerations for security: *prevention*, *detection* and *response*.

Most of the research for secure routing in ad hoc networks has been done in prevention, i.e. the use of cryptographic keys to prevent malicious behavior. Approaches usually require authenticated routing messages. A way to obtain authenticated routing is to use standard digital signatures [2, 3]. For some ad hoc networks with computation, communication or battery constraints, generation and verification of digital signatures is relatively inefficient. SEAD [4] and Ariadne [5] are efficient routing protocols where authenticated routing is achieved without the need of digital signatures (using only symmetric cryptographic primitives).

Intrusion detection systems play a complementary role to that of prevention. First, prevention mechanisms always operate under certain security assumptions. If those assumptions are broken an attacker can bypass the prevention measures, for example SEAD requires distribution of authentic public values to enable authentication of subsequent values. If the authenticity of the public values is broken, SEAD is as insecure as DSDV. Secondly, some attacks are easier to deal with intrusion detection than with prevention mechanisms. For example packet dropping can be easily detected by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving [6]. Prevention of more sophisticated attacks such as a rushing attack or a wormhole is also difficult, thus until efficient prevention mechanisms are designed, an intrusion detection system with signatures or models of the attacks can provide a better cost effective solution.

Third, prevention mechanisms are designed to protect against attacks we know. Anomaly detection can in principle detect unknown attacks.

Any automatic response to a collaborative detection of an attack might be subject to blackmail. So ideally intrusion detection should be used in an environment supporting non-repudiation. To provide non-repudiation we need digital signatures, and thus distributed intrusion detection systems should be implemented only in networks with enough resources.

1.3 Our approach

Our objective is to present a statistical framework that allows the incorporation of prior information about the normal behavior of the network and of network attacks in a principled way for the detection of known and unknown attacks. In order to avoid a large number of false alarms, we have to consider robust statistical models describing a baseline behavior for our feature of interest in MANETs. In contrast to other frameworks that allow anomaly detection [7], we focus on the dynamic behavior of the protocol rather than using static models.

In a highly mobile ad hoc network, as viewed by a monitoring node, the hop count is an important statistic and in most cases can be monitored with no overhead. The evolution of this distribution is directly related to the changes in the topology of the network. Each configuration imposes certain constraints on the space of hop count distributions and as the topology of the network changes from one set of configurations to the next. The space of the configuration can be abstracted and viewed as representing the hidden states of the network and the hop count distribution as the observations.

In terms of the intrusion detection, the basic idea is that an attacker will change the routing information or maliciously modify the routing algorithm in such a way that our perceived evolution of the hop count distribution differs from the its dynamics under the “normal” conditions. When such a deviation persists, in a statistical sense to be described, we declare that an intrusion has occurred. In order to detect the attack as soon as possible we make use of quickest change detection theory.

2 Quickest Detection

Despite the abundance of techniques addressing the quickest detection problem, optimum (non asymptotic) schemes can mostly be found for the case where the observations are independent and identically distributed and the distributions are completely known before and after the change time [8]. However in our case, a model of the dynamics of the hop count distribution should consider that observations depend on past values, so we focus on algorithms that consider this dependency.

2.1 Binary Detection

We follow a cumulative sum (CUSUM) procedure applicable to the case of dependent observations of a stochastic process Y_t, ($t \in \mathbb{N}$, where t is the time index) with densities f_{θ_1}

and f_{θ_0} under hypotheses H_1 and H_0 respectively [9]:

$$S_t = \left\{ S_{t-1} + \log\left(\frac{f_{\theta_1}(y_t|y_{t-1},\ldots,y_k)}{f_{\theta_0}(y_t|y_{t-1},\ldots,y_k)} \right) \right\}^+ \tag{1}$$

where y_k is the first sample after the last reset, i.e., $S_{k-1} = 0$. It is clear that this algorithm is only a reformulation of the sequential probability ratio test (SPRT) algorithm for the log-likelihood ratio: $\log\left(\frac{f_{\theta_1}(y_t|y_{t-1},\ldots,y_k)}{f_{\theta_0}(y_t|y_{t-1},\ldots,y_k)}\right)$ with the lower threshold selected at 0. The upper threshold h will be selected given a false alarm rate.

Anomaly detection is usually cast as a problem of clustering: We first obtain a statistical model f_{θ_0} (a density function in this case) for our "normal" operation. Then we proceed to measure how likely is the observation $f_{\theta_0}(Y_1,\ldots,Y_t)$. If it is below a certain threshold ξ ($f_{\theta_0}(Y_1,\ldots,Y_t) < \xi$), then we declare the observation Y_t an anomaly. In the case of observations in a finite set Ξ, s.t. $|\Xi| = M$, the alternate hypothesis can be considered as the uniform distribution, i.e. $\forall y \in \Xi\,(f_{\theta_1}(y) = 1/M)$. This is a way of not assuming anything about the attack and therefore it is particularly suited for detecting the attacks we do not know of. Equation (1) can now be expressed as

$$S_t = \left(S_{t-1} + \log(1/M) - \log f_{\theta_0}(y_k,\ldots,y_t) + \log f_{\theta_0}(y_k,\ldots,y_{t-1})\right)^+ \tag{2}$$

where $\forall k\,(y_k \in \Xi)$.

3 Statistical model

We build a discrete Hidden Markov Model (HMM) with parameters $\theta = (\pi, A, B)$ for modeling the evolution of hop count distributions. HMMs were selected for several reasons. They provide an generative representation of our system as the hidden states of the HMM can be viewed as abstractions of different spatial configurations of the mobile nodes (figure 1) and the observations as the dynamic evolution of the hop count distribution. The parameters of discrete state HMMs can be specified or can be estimated efficiently while keeping a model with a low bias. The generative and intuitive nature of HMMs allows incorporation of prior knowledge and misuse detection by providing a *language model* [10], i.e. a model that provides the HMM with expert information on allowable state transitions which reflect our knowledge on mobility. Signature-like intrusion detection can also be incorporated by using HMM models of the attacks we already know.

As explained above, we will choose the observations to be the hop count distribution as viewed from a given node (figure 2). For simplicity, we will assume a proactive distance vector routing protocol such as DSDV in order to have access to all hop counts at any time.

If we have $N+1$ nodes, the hop count distribution at the time step k can be considered as a vector in $\{0,\ldots,N\}^D$: $X_k = [X_k^0,\ldots,X_k^{D-1}]'$ ($X_k^i \in \{0,\ldots,N\}$) where D is a limit we impose in the maximum number of hops we will consider, i.e. X_k^0 is the number of disconnected nodes, is X_k^1 the number of nodes 1 hop away, ..., X_k^{D-2} is the number of nodes $D-2$ hops away and X_k^{D-1} is the number of nodes $D-1$ or more hops away.

In order to consider a discrete HMM we need a way to deal with the high-dimensional

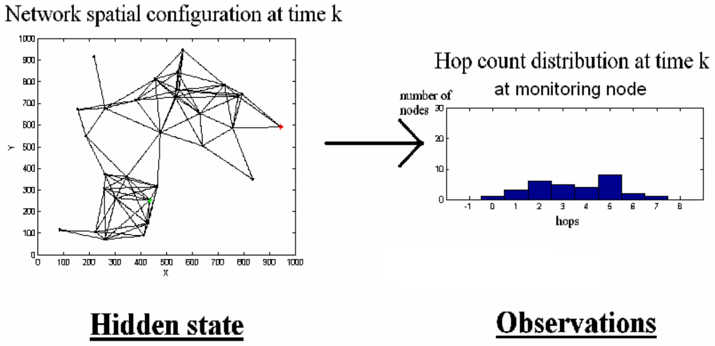

Figure 1: HMM interpretation

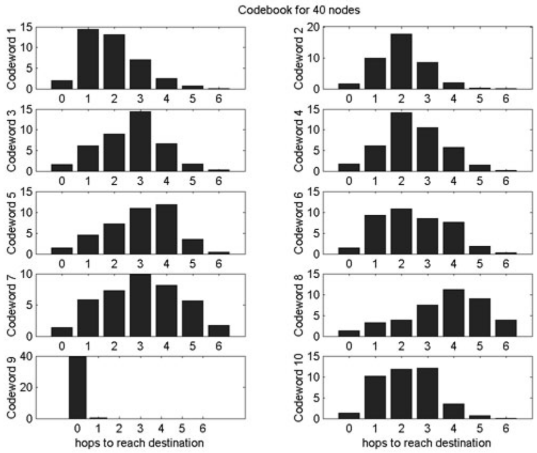

Figure 2: Codebook of size 10 of the hop count distribution for a 40 node ad hoc network

observation vectors X_k. The number of all possible observations is $(N+1)^{D-1}$ since we are working with a hyperplane in $(N+1)^D$ with constraint $\sum_{i=0}^{D-1} X_k^i = N+1$. A natural approach is to encode X_k to Y_k, a member of a set of M codewords. The optimal selection of the codewords is nontrivial and is discussed further in the full version of the paper. One approach to obtain the codebook Ξ is to learn it from the normal operation of the network, by using the classic LBG algorithm in which for a given fixed rate R, we try to find the codebook that minimizes a distortion function (usually a quadratic distortion is considered). Figure 2 shows a codebook of size 10. Learning the codebook from the normal operation has some problems, as discussed in the full version of the paper. Another approach to is to consider a set of M key reference distributions chosen by an expert trying to define what an anomalous behavior can be.

4 Simulation Results

The simulations take place in a 1000x1000m^2 region with 40 nodes moving at speeds of $5m/s$ and with a communication range of $250m$. For the mobility of the nodes, we use the

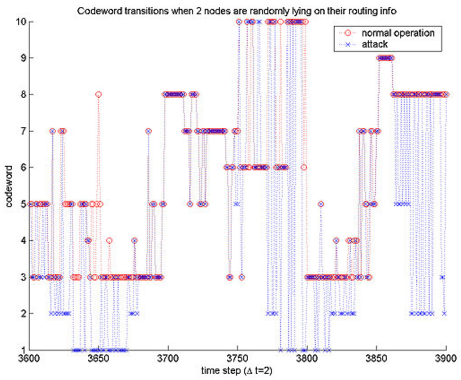

Figure 3: Codeword transitions with two nodes sending bad routing information at random

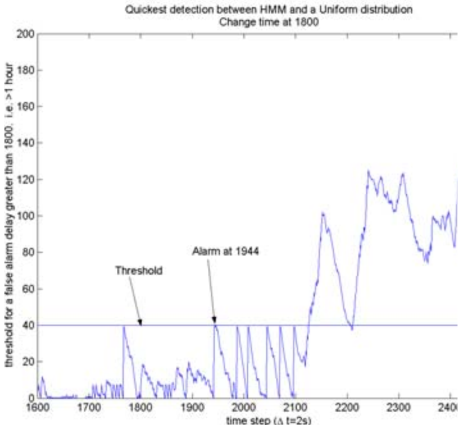

Figure 4: Change detection statistic for attack 1

standard random waypoint algorithm in which the nodes select with a uniform distribution a destination point from the region and after reaching their target they remain there for a given amount of time ($5s$ in our simulation) before selecting another destination. We will be assuming that we monitor one node in which the hop count distribution is sampled every two seconds. A total simulated time of four hours was selected. The HMM is trained with the first 3600 samples. In the following 1800 samples the nodes continue to behave normally and in the final 1800 samples the attack takes place.

A second mobility model considered (avw mobility) is one in a 52x$42m^2$ U-shaped building where there are 47 offices and 47 nodes. Each node spends most of the time in its home office and travels with a speed of $1m/s$ among different offices selected at random. Each node has a communication range of $11m$. A total simulated time of one hour was selected and the time step between measurements was 2 seconds.

The prior is initialized as a uniform distribution. The number of states is selected to be equal to the number of observations and both matrices A_{θ_0} and B_{θ_0} are initialized with higher values in their respective diagonal component than the rest of the values.

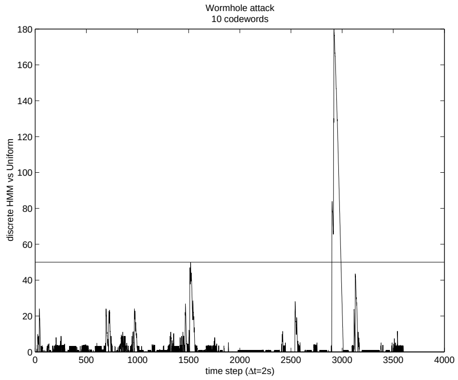

Figure 5: Change detection statistic for a wormhole attack

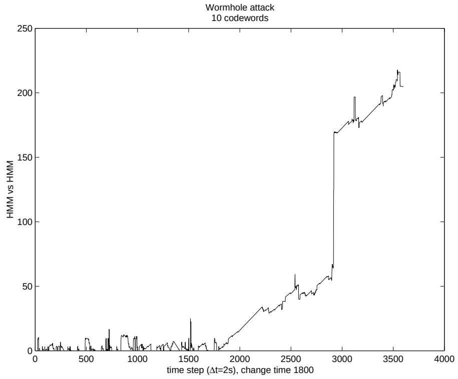

Figure 6: Change detection statistic when we have an HMM model of the attack

The first attack we simulated was an artificial attack to take advantage of the HMM. Under this scenario, two nodes start sending bad routing information randomly at any given time about their distance to any other node. The spurious pattern of the attack caused by the random attack produces more codewords transitions as seen in figure (3). As seen in figure (4), the attack was easily detected using equation (4).

The second scenario considers a wormhole attack, where the endpoints of the wormhole are located at x,y coordinates $(1000/3, 500)m$ and $(2000/3, 500)m$ for the $1000x1000m^2$ plane. This attack was also detected using equation (4). However, we can see in figure 5 that the statistic is not robust to the change.

A way to improve the performance is by including information on the attack. We trained another HMM $(\pi_{\theta_1}, A_{\theta_1}, B_{\theta_1})$ for the attack mode. The resulting performance of this new change detection statistic between two HMMs can be seen in figure 6.

The performance of the change detection statistic for the wormhole attack is similar to an attack in which one node is sending bad routing information constantly. However, in this case, a batch detection procedure by testing the likelihood of the state transitions for a given window of time seems to perform better when we do not have an HMM of the attack. In figure 7 we can see that the state transitions of a normal sequence have on the average a

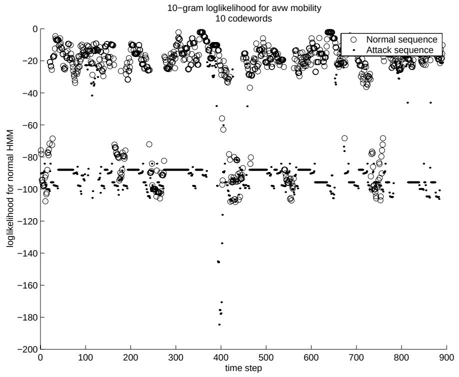

Figure 7: Log-likelihood of state transitions

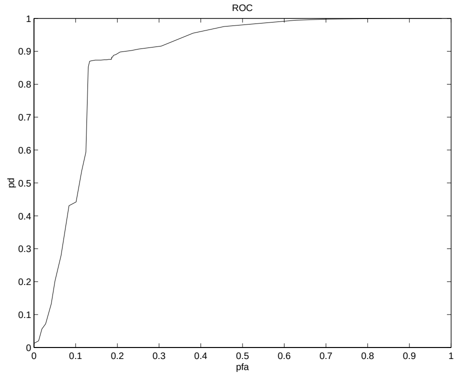

Figure 8: ROC curve for batch detection

higher log-likelihood value than the states transitions from the attack. Figure 8 is the ROC curve.

Another way to deal with the problem is to build a more complex HMM. A natural generalization to avoid the dependence of the detection on the trained codebook is to consider directly the continuous hop count distribution vector $X_k \in \mathbb{R}^D$. To deal with this continuous vector we trained an HMM with a mixture of two Gaussians with two hidden states. With continuous observations we also need a fixed interval in $\mathbb{R}^D$ for defining the uniform probability distribution. However, we decided to estimate the mean of the likelihood $f_{\theta_0}^{GaussianHMM}(x_n|x_{n-1},\ldots,x_k)$ for any new time step x_n, to replace the distribution $\log 1/M$. The resulting performance is shown in figure (9).

5 Conclusions

We presented new approaches to intrusion detection using a statistical framework. For ad hoc networks, our HMMs provide an intuitive model of the network routing behavior, and a principled way for adding expert knowledge in the form of language models or attack models. Simple attacks can be detected by an anomaly detection framework, however, de-

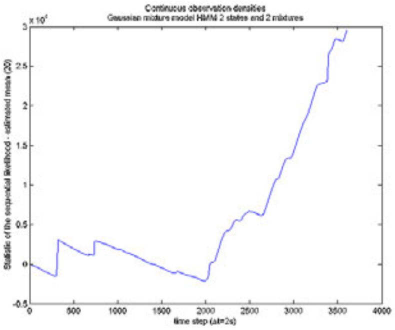

Figure 9: Change detection statistic using a Gaussian mixture output HMM

tection of more complex attacks requires incorporation of prior knowledge into the HMMs. We are working to relax the stationary distribution assumption and deal with distributed detection in the presence of untrusted nodes.

6 Acknowledgments

This material is based upon work supported by the U.S. Army Research Office under Award No. DAAD19-01-1-0494 to the University of Maryland College Park.

References

[1] Y.-C. Hu, A. Perring, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. Technical Report TR01-384, Rice University, December 2001. Revised September 2002.

[2] Manuel Zapata and N. Asokan. Securing ad hoc routing protocols. In ACM Press, editor, *Proceedings of the ACM workshop on wireless security*, pages 1–10, 2002.

[3] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 1999.

[4] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Sead: Secure efficient distance vector routing in mobile wireless ad hoc networks. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA ’02), pages 3–13, June 2002.

[5] Adrian Perrig Yih-Chun Hu and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of MobiCom*, September 2002.

[6] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, pages 255–265, 2000.

[7] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mobile wireless networks. In *ACM/Kluwer Mobile Netowrks and Applications (MONET)*, 2002.

[8] George V. Moustakides. Quickest detection of abrupt changes for a class of random process. *IEEE Transactions on Information Theory*, 44(5), September 1998.

[9] Biao Chen and Peter Willet. Detection of hidden markov model transient signals. *IEEE Transactions on Aerospace and Electronics Systems*, 36(4):1253–1268, October 2000.

[10] R. Rosenfeld. Two decades of statistical language modeling: Where do we go from here. In *Proceedings of the IEEE, 88(8)*, 2000.